UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/001,687	10/23/2001	Dennis Bushmitch	9432-000140	3170

27572 7590 12/01/2006

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 828
BLOOMFIELD HILLS, MI 48303

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 12/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/001,687	BUSHMITCH ET AL.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 August 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10 and 24-67* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10 and 24-67* is/are rejected.

7)☒ Claim(s) *68-71* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on August 31, 2006. Claims 1-10 and 24-71 are currently being considered.

Response to Arguments

2. Applicant's arguments filed August 31, 2006 have been fully considered but they are not persuasive for the following reasons:

Regarding claim 1, the Applicant argues that the Cited Prior Art (CPA), Talton (U.S. Patent Pub. No. 2003/0135739), does not teach a gateway sending a password-specific key to a portable storage device. This argument is not found persuasive. Talton discloses that the user sends a user password to an Authorizer, and if the password is correct, the Authorizer sends key material to the user that is used to decrypt the picks sets on the token (paragraph 16). This key material that is associated with a specific password is interpreted as the "password-specific" key, and this password-specific key is received by the token (portable storage device) and is used to decrypt the pick sets. Therefore, it is respectfully asserted that the CPA does teach a gateway sending a password-specific key to a portable storage device.

In response to the amendments to claims 38, 54, and 67, the 112 2nd paragraph rejections for the claims are removed from the following rejections.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-10 and 24-67 are rejected under 35 U.S.C. 103(a) as being unpatentable over Talton, SR. (U.S. Patent Pub. No. US 2003/0135739) in view of Baize (U.S. Patent No. 6,317,838).

Regarding claim 1, Talton discloses:

A security system for controlling access to a trusted computer network by a client computer, comprising:

a first data store associated with said bastion host and configured to store a set of key-password pairs (paragraphs 15-16), *wherein the token identifier key is interpreted as being the key, and the password is interpreted as being the initial start point*;

a portable storage device (paragraph 9), *wherein the token can be a disk or a smart card*;

a second data store associated with said portable storage device and configured to store passwords represented in said key-password pairs (paragraph 16), *wherein the pick set (set of passwords) is encrypted on the token*;

a user operable initialization mechanism that interfaces with said first and second data stores, said initialization mechanism generating and storing said key-password pairs in said first data store and generating and storing said passwords in said second data store (paragraph 15-16), *wherein the pick sets are generated and the token identifier and the initial start point is stored in the first data store (authorizer) and the passwords (pick sets) are stored on the portable storage device (token);*

an authentication mechanism having a first component associated with said host and having a second component associated with said client computer (paragraphs 17-18), *wherein if the test pick set matches the pick set provided by the user the user is authenticated*;

said first component being configured to communicate a password-specific key associated with one of said key-password pairs to said second component (paragraphs 16-18), *wherein if the password is correctly sent from the user, the Authorizer sends key material to the user so that the pick sets may be decrypted*;

said second component being configured to access said second data store and retrieve at least one password represented in said key-password pair (paragraphs 15-17), *wherein once the pick sets are decrypted, they are sent to the Authorizer for authentication*;

said second component being further configured to communicate said at least one password to said first component based on input from the user and based on said password-specific key communicated from said first component (paragraphs 15-17),

wherein once the pick sets are decrypted, they are sent to the Authorizer for authentication.

Talton does not explicitly disclose a bastion host that controls access to a trusted computer network. Baize discloses a firewall, which filters remote requests to secure access to protected resources (column 3 lines 53-62). Talton discloses that the Authorizer can be used to fetch protected resources or information from a database if the user is authenticated (paragraphs 18-19). Talton and Baize are analogous arts because both use one-time passwords to protect access to resources. The resources of Baize are in a private network protected by a firewall from the insecure Internet. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the bastion host of Baize in conjunction with Talton in situations where the protected resources are being accessed over the Internet to "allow remote users, especially Internet users, to access "friendly" and securely to given private resources protected by a firewall or the like" (column 3 lines 52-55).

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Talton discloses:

The system of claim 1 wherein said portable storage device is a non-volatile memory device (paragraph 9), *wherein the portable storage device can be a disk or a smart card.*

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Baize discloses:

The system of claim 1 wherein said portable storage device is an optical disk (paragraph 9), *wherein the portable storage device can be a disk or a smart card.*

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Talton does not explicitly disclose a screening router system that blocks interaction with said trusted computer network. Baize discloses a screening router system that blocks interaction with said trusted computer network (Figure 1 item 5, column 6 lines 3-9). Talton discloses that the Authorizer can be used to fetch protected resources or information from a database if the user is authenticated (paragraphs 18-19). Talton and Baize are analogous arts because both use one-time passwords to protect access to resources. The resources of Baize are in a private network protected by a firewall from the insecure Internet. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the bastion host of Baize in conjunction with Talton in situations where the protected resources are being accessed over the Internet to "allow remote users, especially Internet users, to access "friendly" and securely to given private resources protected by a firewall or the like" (column 3 lines 52-55).

Claim 7 is rejected as applied above in rejecting claim 6. Furthermore, Talton does not explicitly disclose a screening router system that blocks interaction with said trusted computer network. Baize discloses a screening router system that blocks interaction with said trusted computer network (Figure 1 item 5, column 6 lines 3-9, 33-48). Talton discloses that the Authorizer can be used to fetch protected resources or information

from a database if the user is authenticated (paragraphs 18-19). Talton and Baize are analogous arts because both use one-time passwords to protect access to resources. The resources of Baize are in a private network protected by a firewall from the insecure Internet. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the bastion host of Baize in conjunction with Talton in situations where the protected resources are being accessed over the Internet to "allow remote users, especially Internet users, to access "friendly" and securely to given private resources protected by a firewall or the like" (column 3 lines 52-55). (column 6 lines 33-48).

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Talton discloses:

The system of claim 1 further comprising session management system that restricts interaction with said trusted computer network to an authenticated active session (paragraphs 15-18).

Claim 9 is rejected as applied above in rejecting claim 1. Furthermore, Talton discloses:

The system of claim 1 further comprising session management system that restricts interaction with said trusted computer network to predetermined time duration (paragraphs 15-18).

Claim 10 is rejected as applied above in rejecting claim 1. Furthermore, Baize discloses:

The system of claim 1 further comprising a plug-in module stored on said portable storage device and accessible to said client computer to provide said client computer with instructions in implementing said second component of said authentication mechanism (paragraphs 10, 15-17).

Regarding claim 24, Talton discloses:

A security system comprising:

a device situated between a trusted network and an untrusted network, which stores a set of N password-key pairs, N being an integer greater than one (paragraphs 15-16), *wherein the token identifier key is interpreted as being the key, and the password is interpreted as being the initial start point*;

a portable storage device that stores a set of N encrypted values (paragraph 16), *wherein the pick set (set of passwords) is encrypted on the token*;

a remote client that communicates with said gateway device via the untrusted network and accesses said portable storage device (paragraphs 15-17), *wherein once the pick sets are decrypted, they are sent to the Authorizer for authentication*;

wherein said remote client receives a key of one said set of password-key pairs from said gateway (paragraphs 16-18), *wherein if the password is correctly sent from the user, the Authorizer sends key material to the user so that the pick sets may be decrypted*;

requests an identification value from a user (paragraph 16), *wherein a PIN is entered by the user*;

decrypts a corresponding encrypted value from said set of encrypted values using a combination of said identification value and said key (paragraphs 15-16), *wherein the key material transmitted by the Authorizer is combined with the key material stored on the token to decrypt the pick sets*; and

transmits a result of said decryption to said gateway device (paragraph 17), wherein the pick set is sent to the Authorizer; and

wherein said device authenticates said remote client if said result is equal to a password of said set of password-key pairs (paragraphs 15-17), *wherein once the pick sets are decrypted, they are sent to the Authorizer for authentication*.

Talton does not explicitly disclose a gateway that controls access to a trusted computer network. Baize discloses a firewall, which filters remote requests to secure access to protected resources (column 3 lines 53-62). Talton discloses that the Authorizer can be used to fetch protected resources or information from a database if the user is authenticated (paragraphs 18-19). Talton and Baize are analogous arts because both use one-time passwords to protect access to resources. The resources of Baize are in a private network protected by a firewall from the insecure Internet. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the gateway of Baize in conjunction with Talton in situations where the protected resources are being accessed over the Internet to "allow remote users, especially Internet users, to access "friendly" and securely to given private resources protected by a firewall or the like" (column 3 lines 52-55).

Claim 25 is rejected as applied above in rejecting claim 24. Furthermore, Talton discloses:

The security system of claim 24 wherein said gateway device includes an initialization module that generates said set of password-key pairs (paragraph 15-16), *wherein the pick sets are generated and the token identifier and the initial start point is stored in the first data store (authorizer) and the passwords (pick sets) are stored on the portable storage device (token).*

Claim 26 is rejected as applied above in rejecting claim 24. Furthermore, Talton discloses:

The security system of claim 24 wherein said gateway device includes an initialization module that generates said set of encrypted values (paragraph 16), *wherein the pick sets are encrypted and can only be decrypted by the user's PIN.*

Claim 27 is rejected as applied above in rejecting claim 26. Furthermore, Talton discloses:

The security system of claim 26 wherein said initialization module requests said identification value from the user, and generates said set of encrypted values from said set of password-key pairs (paragraph 16), *wherein the pick sets are encrypted and can only be decrypted by the user's PIN.*

Claim 28 is rejected as applied above in rejecting claim 27. Furthermore, Talton discloses:

The security system of claim 27 wherein said initialization module generates each of said set of encrypted values by encrypting a respective password of said set of password-key pairs with a combination of a respective key of said set of password-key pairs and said identification value (paragraph 16), *wherein the pick sets are encrypted and can only be decrypted by the user's PIN.*

Claim 29 is rejected as applied above in rejecting claim 28. Furthermore, Talton discloses:

The security system of claim 28 wherein said combination of said respective key and said identification value includes a function of said respective key and said identification value encrypted with a symmetric key (paragraph 16), *wherein the pick sets are encrypted and can only be decrypted by the user's PIN.*

Claim 30 is rejected as applied above in rejecting claim 29. Furthermore, Talton discloses:

The security system of claim 29 wherein said function is a bitwise exclusive-or (paragraph 16), where using an XOR function to combine data was well-know in the art at the time of invention.

Claim 32 is rejected as applied above in rejecting claim 24. Furthermore, Talton discloses:

The security system of claim 24 wherein said gateway device filters out all packets bound for the trusted network, except for packets from said remote client once said remote client has been authenticated by said gateway device (paragraphs 16-18), wherein if the pick sets don't match, the request is not authorized and thereby dropped.

Claim 33 is rejected as applied above in rejecting claim 24. Talton does not explicitly disclose that the gateway device revokes authentication after a predetermined period. Baize discloses that one time passwords change on a regular basis based on predetermined periods (column 7 lines 45-61). Talton and Baize are analogous in that both use one-time passwords. It would have been obvious to use expiring passwords in the system of Talton so that the passwords "can not be "replayed"" (column 3 lines 27-33).

Claim 35 is rejected as applied above in rejecting claim 24. Furthermore, Talton discloses:

The security system of claim 24 wherein said combination of said identification value and said key includes a function of said key and said identification value encrypted with a symmetric key (paragraph 16), *wherein the pick sets are encrypted and can only be decrypted by the user's PIN.*

Claim 37 is rejected as applied above in rejecting claim 24. Furthermore, Talton discloses:

The security system of claim 24 wherein said gateway device uses said set of password-key pairs at most once (paragraph 13).

Claim 38 is rejected as applied above in rejecting claim 24. Furthermore, Talton discloses:

The security system of claim 24 wherein said gateway device includes an initialization module that generates said set of password-key pairs and said set of encrypted values, and stores said set of encrypted values into said portable storage device when said portable storage device within a perimeter of said trusted network (paragraphs 15-16).

Claim 39 is rejected as applied above in rejecting claim 24. Furthermore, Talton discloses:

The security system of claim 24 wherein said portable device is associated with a user identifier, said remote client communicates said user identifier to said gateway device, and said gateway stores a set of password-key pairs for each user identifier (paragraphs 15-17).

5. Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over Talton, SR. (U.S. Patent Pub. No. US 2003/0135739) in view of Baize (U.S. Patent No. 6,317,838) in further in view of Rasmussen et al. (U.S. Patent No. 5,301,247).

Claim 31 is rejected as applied above in rejecting claim 24. Talton does not explicitly disclose wherein each password-key set is numbered and associated with an index number i, said gateway sending the index number to the remote client to select the set of encrypted values. Rasmussen discloses a table entry associated with a key being sent to a remote station to determine which key is to be retrieved from the key table (column 2 lines 57-65). Talton, Baize and Rasmussen are analogous arts in that all of them delineate a key exchange between a remote station and another station for the purposes of secure and authenticated communication. It would have been obvious to one of ordinary skill in the art at the time of invention to use the key table entry to determine which key is to be retrieved so that the keys can be quickly determined and if the received key table entry value does not match to determine an error (column 2 lines 57-65).

6. Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over Talton, SR. (U.S. Patent Pub. No. US 2003/0135739) in view of Baize (U.S. Patent No. 6,317,838) in further in view of Feit et al. (U.S. Patent Pub. No. US 2001/0056354 A1).

Claim 34 is rejected as applied above in rejecting claim 24. Talton-Baize disclose a connection between a remote client and a server/gateway, but do not explicitly disclose that the connection is a SSL connection. Feit discloses a SSL connection between a client (remote device) and a web server (gateway) (paragraph 40). It would have been obvious to employ SSL as in Feit in the system of Talton-Baize to "add security to such a connection" (paragraph 40) and to "provide a remote user a secured channel for transmitting data over the Internet (paragraph 40).

7. Claims 40-55 are method claims analogous to the system claims 24-39 rejected above, and therefore, are rejected following the same rationale.

8. Claims 56-67 are device/apparatus claims analogous to the system claims 24-39 rejected above, and therefore, are rejected following the same rationale.

Allowable Subject Matter

9. Claims 68-71 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KA
11/22/2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100